

CLERK'S OFFICE

A TRUE COPY

Mar 03, 2022

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the accounts of lebronfuture24@icloud.com
that is stored at premises owned, maintained, controlled, or operated by
Apple Inc., as further described in Attachment A.

Case No. 22 MJ 9

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

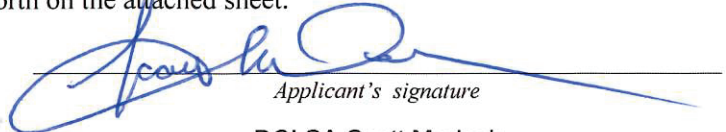
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841 and 846	Distribution and possession with intent to distribute, and conspiracy to distribute and possess with the intent to distribute controlled substances.
18 U.S.C. § 924(c)	Possession of a firearm in furtherance of a drug trafficking crime.

The application is based on these facts:
See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of _____ days (give exact ending date if more than 30 days: 03/03/2022) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



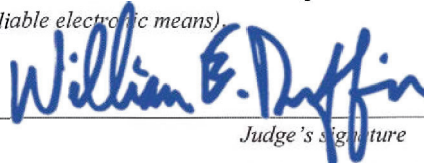
Applicant's signature

DCI SA Scott Marlock

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means)

Date: 3/3/2022



Judge's signature

City and state: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Scott Marlock, being first duly sworn, hereby depose and state as follows:

I. BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – electronic devices – which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the State of Wisconsin Department of Justice, Division of Criminal Investigation (DCI) and have been employed by DCI for the past 2 years. Prior to DCI, I was employed by the Milwaukee Police Department (MPD) for approximately 27 ½ years and retired from MPD in March of 2020. I am also currently assigned to the Milwaukee Office of the United States Department of Justice, Drug Enforcement Administration (DEA) as a Task Force Agent and have been federally deputized for the past 10 years. I have specialized training and experience in narcotics smuggling and distribution investigations as well as financial investigations. During my tenure with MPD and DEA, I have participated in over 500 narcotics investigations and financial investigations and have authored over 100 affidavits supporting criminal complaints and search and seizure warrants. I have debriefed more than 100 defendants,

informants, and witnesses who had personal knowledge regarding major narcotics trafficking and money laundering organizations.

3. In connection with my official DCI and DEA duties, I investigate criminal violations of the federal controlled substance laws, including, but not limited to Title 18, United States Code, Sections 924(c), 1956 and 1957, Title 21, United States Code, Sections 841, 843, 846, 952, and 963.

4. The information set forth in this affidavit comes from my personal involvement in this investigation, as well as from information provided to me by other law enforcement officers, who were directly involved in the matter or have personal knowledge of the facts herein. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

II. PROBABLE CAUSE

1. Beginning in January of 2022, a confidential informant (CI) made

statements to case agents regarding the CI's source of fentanyl. The CI advised s/he had been obtaining fentanyl from "Courtney," (subsequently positively identified as Keshawn AIKENS) since approximately September of 2021 approximately 2-3 times per week. The CI stated s/he started by obtaining 1.5 grams of fentanyl from AIKENS per meeting however, that amount quickly increased. The most fentanyl the CI obtained at one time from "Courtney" aka AIKENS was 35 grams.

2. Case agents believe the CI is credible and reliable because beginning in January of 2022, a confidential informant (CI) made statements against the CI's penal interest. The CI is cooperating in exchange for consideration on a pending state narcotics case. Thus far, the information provided by the CI has been corroborated by independent information known to case agents gathered during the course of this investigation. According to law enforcement databases, the CI has no felony or misdemeanors convictions.

3. The CI advised s/he communicates with "Courtney" aka AIKENS, via telephone at (414) 313-4340 (Target Telephone) and that Courtney has had that number for several months. The CI typically sent a text message to Courtney at the Target Telephone asking if s/he could meet to purchase fentanyl. The CI would also text Courtney once the CI was approximately 30 minutes from their pre-determined meeting location, which most recently had been behind the Walgreens located at 7171 N. Teutonia Avenue, Milwaukee, WI.

4. On January 13, 2022, at the direction of law enforcement, the CI sent a text

message to "Courtney," aka Keshawn AIKENS at (414) 313-4340 and inquired if the CI could meet Courtney in order to purchase fentanyl. Courtney replied, "Yup." Case agents met with the CI at a pre-determined location. A search of the CI and the CI's vehicle was conducted for any weapons, contraband, or large sums of US currency with none being located. Case agents provided the CI with \$1,200 in pre-recorded US currency as well as an audio/video recording/transmitting device. Case agents followed the CI from the pre-determined location directly to Walgreens where the CI parked. Case agents maintained a constant visual of the CI and the CI's vehicle.

5. Numerous additional text messages were exchanged between the CI and "Courtney" aka Keshawn AKIENS including one in which the CI informed AIKENS that the CI was behind Walgreens, 7171 N. Teutonia Avenue, Milwaukee, WI. Courtney replied, "Ok I'm coming down good hope now." At approximately 1:46 p.m., a silver Land Rover bearing WI registration AMU-9598 arrived and parked near the CI's vehicle. The CI exited the CI's vehicle, entered the Land Rover. Shortly thereafter, the CI exited the Land Rover and departed the area. The Land Rover also departed the area.

6. Case agents followed the CI directly from Walgreens, 7171 N. Teutonia Avenue to a pre-determined location. Upon arrival, the CI turned over to case agents a knotted plastic sandwich bag containing an off-white chunky substance, suspected to be fentanyl. The CI advised that once the Land Rover arrived the CI entered and provided the \$1,200 in pre-recorded US currency to AIKENS, aka "Courtney," who was the driver and sole occupant. AIKENS then provided the CI with the suspected fentanyl in the

knotted plastic sandwich bag.

7. A subsequent query of the WI Department of Transportation revealed the AMU-9598 was registered on a silver 2018 Land Rover, VIN: SALYB2RX6JA733635, to Jasmine R. Ransaw (DOB: 06/07/1990) at 2745 N. 8th Street, Milwaukee, WI.

8. Case agents later transported the suspected fentanyl to the DCI-Milwaukee Field Office and subjected a sample of it to a Mecke's Modified Reagent #11 field test. Results of this test revealed a positive indication for the presence of opiates. In addition, the suspected fentanyl weighed approximately 29.2 grams in its packaging.

9. On January 13, 2022, case agents conducted a check of the social media site Facebook page of Jasmine Ransaw and observed that the individual depicted in the profile picture of Ransaw was the same as the person depicted in the WI Department of Transportation driver's license photograph of Jasmine R. Ransaw (DOB: 06/07/90). On January 5, 2022, Ransaw re-posted a post from the Facebook account of "Keshawn AIKENS." The post from AIKENS contained two photographs of a black male with extremely white teeth and matching the description the CI provided of "Courtney." SA Hepp showed these photographs to the CI and the CI believed this male was in fact the person s/he knew as "Courtney."

10. On January 13, 2022 case agents confirmed that the individual depicted in a majority of the Facebook profile pictures of Keshawn Aikens was the same as the person depicted in the WI Department of Transportation driver's license photograph of Keshawn D. AIKENS (DOB: 01/20/97).

11. On January 27, 2022, at the direction of law enforcement, the CI placed a recorded and monitored call to Aikens at the Target Telephone and inquired if the CI could meet AIKENS in order to purchase 15 grams of fentanyl. AIKENS asked, "For how much?" The CI reiterated "15," and AIKENS replied, "Alright."

12. Case agents met with the CI at a pre-determined location. A search of the CI and the CI's vehicle was conducted for any weapons, contraband, or large sums of US currency with none being located. Case agents provided the CI with \$900 in pre-recorded US currency as well as an audio/video recording/transmitting device. Case agents followed the CI from the pre-determined location directly to Walgreens where the CI parked. Case agents maintained a constant visual of the CI and the CI's vehicle.

13. Additional text messages were exchanged between the CI and the Target Telephone including one in which the CI informed AIKENS that the CI was behind Walgreens, 7171 N. Teutonia Avenue, Milwaukee, WI. AIKENS replied, "Ok making my way".

14. Case agents observed the Land Rover ("Target Vehicle") exit the parking garage of 11011 W. North Avenue and traveled to Mayfair Mall where the driver and sole occupant, a black male, exited and walked into the mall. A short time later, this same individual re-entered the Target Vehicle. Case agents followed the Target Vehicle directly from Mayfair Mall to Walgreens at 7171 N. Teutonia Avenue and parked near the CI's vehicle. The CI exited the CI's vehicle and entered the Target Vehicle. A short time later, the CI exited the Target Vehicle and departed the area. The Target Vehicle also

departed the area.

15. Case agents followed the CI directly from Walgreens, 7171 N. Teutonia Avenue to a pre-determined location. Upon arrival, the CI turned over to case agents a knotted plastic sandwich bag containing an off-white chunky substance, suspected to be fentanyl. The CI advised that once the Target Vehicle arrived the CI entered and provided the \$840 in pre-recorded US currency to AIKENS who was the driver and sole occupant. AIKENS then provided the CI with the suspected fentanyl in the knotted plastic sandwich bag.

16. Case agents later transported the suspected fentanyl to the DCI-Milwaukee Field Office and subjected a sample of it to a Nark II Fentanyl Reagent field test. Results of this test revealed a positive indication for the presence of fentanyl. In addition, the suspected fentanyl weighed approximately 26.2 grams in its packaging.

17. Surveillance followed the Target Vehicle directly to a Target store, 3900 N. 124th Street, Wauwatosa, WI, at which time AIKENS exited the driver's seat and entered Target. SA Novak followed AIKENS into Target and confirmed AIKENS' identity from having previously viewed photographs of Aikens.

18. A short time later, AIKENS exited Target and departed the area in the Target Vehicle. Surveillance units followed until it pulled into the gas station at 12324 W. North Avenue, Wauwatosa, WI. AIKENS exited the Target Vehicle and SA Hepp positively identified him as AIKENS, based on his familiarity with this investigation as well as having previously viewed photographs of AIKENS.

19. Aikens eventually departed the gas station in the Target Vehicle. Surveillance units followed the Land Rover directly to the Mayfair Reserve apartments at 11011 W. North Avenue, Wauwatosa, WI. Case agents observed the Target Vehicle pull into the parking structure for the apartments.

20. On February 2, 2022, case agents conducted physical surveillance at the Mayfair Reserve apartments, 11011 W. North Avenue, Wauwatosa, WI and electronic surveillance (obtained via state court tracking warrants) of the Target Vehicle and the Target Telephone, both of which are known to be utilized by AIKENS.

21. At approximately 4:03 p.m. case agents observed the Target Vehicle pull into the parking structure of 11011 W. North Avenue. SAs Novak and Hepp walked to the hallway in the immediate vicinity of apartment #222. At approximately 4:06 p.m. case agents observed AIKENS utilize keys to unlock and enter apartment #222. Case agents also observed the Land Rover in the 2nd story of the parking structure, immediately inside the door to access the interior, not in its assigned parking spot (#221). Case agents believed AIKENS parked right next to the door because he would be leaving again soon.

22. On February 9, 2022, at approximately 3:31 p.m. case agents noted that the data pertaining to the location of AIKENS' telephone, (414) 313-4340, revealed that it was in the immediate vicinity of 11011 W. North Avenue, Wauwatosa, WI. At this same time, data pertaining to the Land Rover AIKENS is known to drive (AMU-9598, WI) revealed it was parked near 2745 N. 8th Street, Milwaukee, WI. At approximately 3:31 p.m. case

agents checked the area of the apartments at 11011 W. North Avenue and observed a white Jeep Grand Cherokee bearing WI registration ANT-4357 parked in front of the lobby for the apartments. Due to the tinted windows on the Jeep, SA Hepp was only able to determine that the driver's seat was occupied by either a B/M or a B/F. At approximately 3:33p.m. the Jeep departed the area. A subsequent query of the WI DOT revealed ANT-4357 was registered to AIKENS on a 2020 Jeep Grand Cherokee, white, VIN: 1C4RJFDJ4LC757500.

23. Case agents reviewed data pertaining to the location of the Target Telephone. From the date case agents began receiving this data, January 25, 2022, through February 11, 2022, the Target Telephone was in the immediate vicinity of 11011 W. North Avenue, Wauwatosa, WI every day at 3:00 a.m., a time people are generally sleeping.

24. In the morning hours of February 11, 2022, data pertaining to the location of Keshawn AIKENS' telephone (414) 313-4340, and his vehicle, a 2018 Land Rover Velar (AMU-9598 WI), revealed both were at his apartment, 11011 W. North Avenue, Wauwatosa, WI. At approximately 10:00 a.m. case agents observed the Land Rover in its assigned parking spot, #221, inside the apartment's garage.

25. At approximately 10:59 a.m. case agents observed AIKENS exit his apartment, Unit #222, and walk toward the parking garage. A short time later AIKENS was observed by members of the Wauwatosa Police Department walking toward the Land Rover in the garage. At the request of SA Hepp, these members of the Wauwatosa

PD took AIKENS into custody based on probable cause for two counts of Manufacture/Delivery of Schedule II (Fentanyl).

26. As Aikens was taken into custody, a handgun fell onto the ground from Aikens' waistband. DCI SA Hepp recovered this handgun and observed it was a Glock Model 45, 9mm, S/N BRKS858. SA Hepp discovered it was loaded with a live round in the chamber and 13 live rounds in the inserted magazine.

27. During the search of AIKENS incident to his arrest, DCI SA Hepp recovered an iPhone in a blue case recovered from Aikens' hand (Device A); an iPhone in a gold/blue case found in Aikens' jacket pocket (Device B); a clear plastic knotted sandwich containing an off-white chunky substance suspected to be fentanyl recovered from Aikens' left front pants pocket; \$80 in US currency recovered from Aikens' left front pants pockets; and a ring of keys containing a fob for the Land Rover, a fob for a Dodge, multiple fobs for residential/apartment doors, and other standard keys for residential doors.

28. Case agents later subjected a sample of the suspected fentanyl to a Nark II Fentanyl Reagent field test. This test revealed a positive indication for the presence of fentanyl. SA Hepp weighed the evidence utilizing a non-certified electronic scale and found the evidence to weigh approximately 51.7 grams in its original packaging which consisted of a clear knotted plastic sandwich bag.

29. While waiting to obtain a federal search warrant for the residence, including the search of all cell phones located in the residence, case agents maintained

surveillance of 11011 W. North Avenue, Apartment #222 Wauwatosa, WI, and secured the residence. During that surveillance, case agents observed AIKENS' girlfriend, Crystal Q. Jester, exit Apartment # 222 holding a gold iPhone with a cracked screen protector in a gold/clear case (Device C). Jester was detained by case agents and was told that her boyfriend, AIKENS, had been arrested and that case agents were waiting for a search warrant for the residence. Given that case agents were waiting for a federal search warrant for all cell phones located in the residence and Jester had exited with a cell phone, case agents seized Jester's cell phone based upon probable cause that it may have been used by AIKENS. Jester stated it was her cell phone and provided a passcode to case agents to look something up on her phone for her. Case agents maintained custody of Device C.

30. The Honorable James R. Sickel, United States Magistrate, Eastern District of Wisconsin, signed a search warrant authorizing a search of Aikens' apartment, 11011 W. North Avenue, Unit #222, Wauwatosa, WI 53226. At approximately 1:01 p.m. case agents executed the knock and announce search warrant at AIKENS' and Jester's residence. Case agents knocked and announced police presence and ordered anybody inside the apartment to come to the door. Nobody from inside the apartment responded for more than 30 seconds, therefore agents made entry into the apartment utilizing a key obtained from Jester's key ring. Case agents did not locate any other people inside the apartment. Agents then conducted a search of the apartment

31. In the lower cabinet to the north of the stove, case agents located four plastic

baggies, each of which contained an off-white powdery/chunky substance, suspected to be fentanyl (further described below); a hydraulic drug press, a bag of Inositol a blender, sandwich baggies with residue, white vinegar, a spray bottle, vice grips, a hot pad with residue, plastic cups, a screwdriver, a hammer, two digital scales, and a strainer. Case agents are aware that these items are commonly used in conjunction to adulterate fentanyl to increase its volume as well as to package the fentanyl for sales.

32. Case agents later weighed the above-mentioned suspected fentanyl: a) a knotted sandwich bag containing tan chunky/powdery substance, approx. 57.6 grams in packaging, b) a clear plastic Ziploc bag containing tan chunky/powdery substance, approx. 79.9 grams in packaging, c) a knotted sandwich bag containing tan chunky/powdery substance, approx. 6.0 grams in packaging, d) an unknotted sandwich bag containing tan chunky/powdery substance, approx. 3.4 grams in packaging. SA Hepp subjected a sample of the substance from item b) to a Nark II Fentanyl Reagent field test. Results of this test revealed a positive indication for the presence of fentanyl

33. On the kitchen counter case agents located miscellaneous documents addressed to AIKENS as well as a bag of small rubber bands, commonly used to bundle large sums of US currency.

34. In the top drawer of the bedroom's south nightstand, case agents recovered the following items: a WI Certification of Title for a 2020 Jeep, VIN: 1C4RJFDJ4LC757500; a WI ID card for AIKENS; a black plastic case for a Glock G45 9mm handgun, S/N BRKS858; a case for a Glock model G17 S/N BNMV276; a box of "norma" band 9mm

luger ammunition containing 17 live rounds; a jewelry appraisal for a "10k yellow gold heavy link chain, weighing approx. 313.2 grams set with round brilliant cut diamonds weighing approx. 30.62 carats total weight, G color and VVS1-VS2 clarity, pave set: Insurance Replacement Value: \$43,900 (from Shabtai Trading Inc, Chicago, IL); a receipt for a ring set with natural diamonds in 10k yellow gold, weighing 32.232 gms: \$6,500 paid for in cash (from Majestic Jewelers, Chicago, IL); an SS Datejust watch: \$7,650 + tax = \$8,070.75 paid for in cash (from Schwanke-Kasten Jewelers, Whitefish Bay, WI); a Milwaukee County Court summons addressed to Aikens; a Milwaukee Municipal traffic citation notice addressed to Aikens; and a WI DOT "Confirmation of Ownership" regarding Land Rover (VIN:SALYB2RX6JA733635) titled to Jasmine Ransaw.

35. In the bottom drawer of the bedroom's south nightstand, case agents recovered approximately \$71,000 in US currency.

36. In a plastic bin on the floor of the bedroom closet case agents recovered numerous documents addressed to Jester.

37. Underneath the bathroom sink case agents recovered a money counter.

38. In the left cabinet of television stand in the living room, case agents recovered additional US currency. Once the search of the residence was completed, the apartment was re-secured with the aforementioned key. Agents left the residence at approximately 2:17 p.m. A copy of the search warrant was left inside the apartment.

39. At approximately 3:38 p.m. case agents conducted a recorded interview of Aikens while at the Wauwatosa Police Department. DCI SA Hepp advised AIKENS of

his Miranda rights and AIKENS indicated he was willing to answer questions. Aikens advised he “made bad decisions” and that he was “willing to take responsibility” for what case agents found on him and on his apartment. Aikens said he tried to keep his drug activity away from Jester and said he did not want to get anyone else involved.

40. AIKENS claimed that he began selling narcotics “a few months ago.” Aikens said he did not know the people he sold narcotics to and that he did not sell to too many people. Aikens said he dropped out of high school during his senior year and has not been employed since 2016.

41. Regarding the firearm recovered from Aikens, he advised that he was shot in approximately 2017 and therefore carries the handgun for personal protection. AIKENS’ confirmed the handgun was his.

42. While SA Hepp transported Aikens to the Milwaukee County Jail, Aikens suggested that SA Hepp could have \$25,000 of the money recovered from Aikens’ nightstand as long as SA Hepp returned the remaining money to Aikens. Once at the jail, Aikens repeated this same offer to Inv. Haese. In addition, while at the jail, Aikens informed SA Hepp that in 2021 Aikens spent \$110,000 on clothing and other items.

43. On February 17, 2022 the Honorable Nancy Joseph, United States Magistrate, Eastern District of Wisconsin, signed a search warrant authorizing a search of Devices A, B, and C. Device B was passcode protected however a forensic examination revealed Device B was assigned telephone number (414) 313-4340 and was associated with an iCloud account of lebronfuture24@icloud.com. In addition, the contents of the

telephone were last backed up to the iCloud account on February 10, 2022 and approximately 11:07 p.m., which was the evening before the arrest of Aikens.

44. On February 23, 2022 the case against Aikens was presented to a federal grand jury in the Eastern District of Wisconsin. This grand jury returned a true bill, securing the indictment Aikens on one count of Possession with Intent to Distribute 40 grams or more of a substance containing fentanyl, and one count of Possession of a Firearm in Furtherance of a drug trafficking crime.

45. Based on the above information and facts, I submit that there is probable cause to believe the iCloud account lebronfuture24@icloud.com contains evidence that Aikens has violated the laws of the United States, in that he distributed fentanyl, a Schedule II controlled Substance, possessed with intent to distribute fentanyl, a Schedule II substance, and possessed a firearm in furtherance of his possession with intent to distribute fentanyl, a Schedule II controlled substance, all in the Eastern District of Wisconsin.

INFORMATION REGARDING APPLE ID AND ICLOUD¹

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

65. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

66. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices,

and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and

television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

67. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

68. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

69. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition,

Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

70. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

71. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"),

and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

72. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

73. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

74. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. For example, these communications and files may include, among other things, text messages or screen shots of text messages between Aikens, his narcotics customers, and his co-conspirators, records of financial transactions of proceeds from Aikens’ narcotics trafficking crimes, and photographs evidencing his narcotics trafficking activities. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of the kind of criminal activity described herein, including to communicate and facilitate the offenses under investigation.

75. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be

evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

76. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

77. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators, or applications used to post ads for prostitution, conduct financial transactions with proceeds of sex trafficking, and/or make reservations for travel and hotels used for sex trafficking activities. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

78. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including, but not limited to, information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

79. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the accounts of lebronfuture24@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A;

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses,

Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from October 1, 2021 to the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from October 1, 2021 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All activity and transactional logs related to attempts to erase or restore the account or devices connected to the account to factory settings;

h. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

i. All records pertaining to the types of service used;

j. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

k. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **7 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §924(c) and 21 U.S.C. §841(a)(1) and 841(b)(1)(B) involving Keshawn D. Aikens since October 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;
- f. Evidence of communications between the subscriber and his drug trafficking customers and/or co-conspirators;

- g. Evidence indicating how and where the subscriber spent and stored the proceeds of his illegal drug trafficking;
- h. Evidence of the execution of the subscriber's criminal activity.